DELINCUENCIA INFORMATICA

La comprensión de conductas que abren las puertas a la delincuencia informática permitirá perfeccionar las técnicas preventivas y la protección de los usuarios

Lorrie Faith Cranor

CONCEPTOS BASICOS

La "ciberpesca", o *phishing*, es una forma de delito informático que incita a facilitar información reservada de carácter personal o empresarial. Constituye una forma de timo que cada año le detrae miles de millones de euros a sus víctimas.

Dado que la ciberpesca depende de acciones de los usuarios de sistemas informáticos, el estudio de los motivos que llevan a picar en esta clase de cebos puede contribuir a perfeccionar las técnicas de lucha contra la ciberpesca y la mejor formación de los usuarios.

Para anular o reducir la ciberpesca es imprescindible que los agentes de la ley, los expertos en seguridad informática y los propios usuarios aúnen sus esfuerzos.

Llevo semanas recibiendo mensajes y correos electrónicos remitidos por bancos, advirtiéndome de que los servicios "en línea" de que dispongo corren el riesgo de quedar desactivados; mensajes de eBay diciéndome que he de utilizar una nueva contraseña; de Apple, que me reclama deudas pendientes por descargas de música; de unas líneas aéreas, que me ofrecen la oportunidad de ganar rápidamente 50 euros por cumplimentar una encuesta, y de la Cruz Roja, solicitándome un donativo para las víctimas de la guerra en el Congo.

Todos esos mensajes son muy convincentes, y parecen auténticos. Pero, a excepción del mensaje remitido por eBay, todos son fraudulentos: correos electrónicos de los conocidos en la jerga por *phish*, esto es, mensajes-cebo para "ciberpesca".

Los correos electrónicos de ciberpesca son cebos elaborados por artistas del timo, concebidos para hacerlos pasar por comunicaciones legítimas, que, a menudo, parecen remitidas por entidades de renombre y de buena reputación. En general, se les solicita a las posibles víctimas que actúen sin demora, para evitar inconvenientes o recibir alguna recompensa. La respuesta esperada suele consistir en que la víctima entre en alguna página de la Red, o llame a un número de teléfono, y facilite información personal. En otras ocasiones, basta con que las víctimas "pinchen" en algún enlace o abran documentos adjuntos de los correos electrónicos para que sus ordenadores queden infectados por programas maliciosos —*malware*— que permiten a los *phishers*, o ciberpescadores, apoderarse de datos que desean, o incluso hacerse con el control del ordenador de la víctima para lanzar desde él futuros ataques.

Los detalles de los cebos difieren de un caso a otro. Lo que no empece que el resultado sea el mismo: millares de víctimas confiadas o desprevenidas le facilitan información a delincuentes, que éstos utilizan después para abrirse paso hasta sus cuentas bancarias y saquearlas, para suplantar su identidad o para ambas cosas.

El Anti-Phishing Working Group es un consorcio internacional de organizaciones dedicadas a eliminar timos y transacciones fraudulentas por Internet. Entre otras actuaciones, este grupo de trabajo rastrea las actividades de "pesca informática", y procura determinar cada mes el número de sedes de la Red que se dedican a ella. En 2007, los totales mensuales llegaron a sumar 55.643. En cada uno de esos meses, fueron utilizadas como cebo entre 92 y 178 marcas o empresas de diversas categorías, lo que significa que sus emblemas o distintivos fueron utilizados para hacer creer a las víctimas que estaban tratando con instituciones de confianza. Gartner, una firma de investigación y asesoría, estima que unos 3,6 millones de norteamericanos fueron víctimas del timo, con pérdidas que suman en torno a 2500 millones de euros.

Siendo de tal volumen las cifras en juego, la comunidad de seguridad informática se ha aprestado a desarrollar técnicas para combatir la ciberpesca, entre las que se cuentan los filtros de correo y los navegadores que denuncian tentativas de *ciberpesca*. Estos programas han contribuido, sin duda, a bloquear muchos ata-